Seguridad y privacidad en internet

Pese a ser dos conceptos distintos, Seguridad y Privacidad van íntimamente relacionados. Conocer y aplicar normas de seguridad en internet, nos permitirá mantener a salvo nuestra privacidad y la de nuestra información.

A continuación, vamos a ver una serie de consejos para mantener a salvo nuestra privacidad:

Contraseñas seguras y robustas:

> Una de las primeras barreras más importantes para evitar el uso fraudulento de nuestra identidad es tener una contraseña robusta y difícil de descifrar. Aquí te ponemos algunas características que una contraseña debería tener para responder a los criterios mínimos de seguridad.

1. CUALIDADES QUE DEBERÍA CUMPLIR UNA CONTRASEÑA:

- **Debemos asegurarnos que la contraseña tenga** una:
  - longitud mínima de doce caracteres,
  - que combine mayúsculas,
  - minúsculas,
  - números y
  - símbolos.
- **No debemos utilizar como claves:**
  - palabras sencillas en cualquier idioma,
  - nombres propios,
  - lugares,
  - combinaciones excesivamente cortas,
  - fechas de nacimiento,
  - etc.
- **Tampoco debemos usar claves formadas únicamente a partir de la concatenación de varios elementos**. Por ejemplo: “Juan1985” (nombre + fecha de nacimiento).

2. CUALIDADES QUE UNA CONTRASEÑA NO DEBERÍA TENER

Ejemplo de cómo deben ser las contraseñas

Oficina de seguridad del internauta. Imagen monográfico que deberías saber contraseñas ejemplos. https://www.osi.es/sites/default/files/quedeberiassaber/imagen-monografico-que-deberias-saber-contrasenas-ejemplos.png

> Dentro de este artículo *https://www.osi.es/es/contrasenas* hacen el siguiente análisis de **cuanto tardaría un software** de combinación de caracteres en adivinar una contraseña **dependiendo de la combinación** que realizamos con los caracteres. Por un lado sería mezclando mayúsculas y minúsculas (todos los caracteres) y por otro solo minúsculas:

Longitud	Todos los caracteres	Sólo minúsculas
3 caracteres	0,86 segundos	0,02 segundos
4 caracteres	1,36 minutos	0,46 segundos
5 caracteres	2,15 horas	11,9 segundos
6 caracteres	8,51 días	5,15 minutos
7 caracteres	2,21 años	2,23 horas
8 caracteres	2,10 siglos	2,42 días
9 caracteres	20 milenios	2,07 meses
10 caracteres	1.899 milenios	4,48 años
11 caracteres	180.365 milenios	1,16 siglos
12 caracteres	17.184.705 milenios	3,03 milenios
13 caracteres	1.627.797.068 milenios	78,7 milenios
14 caracteres	154.640.721.434 milenios	2.046 milenios

https://www.osi.es/es/contrasenas

Estrategias para generar contraseñas

Una vez visto que cualidades debe cumplir una contraseña para ser segura, vamos a ver diferentes estrategias para que además de ser segura también sea fácil de recordar y útil para nosotros. Es importante que cualquier **contraseña siga un proceso cognitivo lógico** para que si no recordamos exactamente los elementos de la contraseña, mediante el razonamiento lógico seamos capaces de deducirla.

> Es aconsejable utilizar **contraseñas diferentes para las diferentes plataformas** que utilicemos, ya que si se produce un grieta de seguridad en alguna de nuestras cuentas y quedamos descubiertos, estas credenciales servirían para poder entrar en el resto de cuentas.

En ocasiones, recordar todas las contraseñas que utilizamos (correo electrónico, redes sociales, mensajería instantánea, foros, etc.) puede resultar complicado. Para facilitar la tarea, podemos utilizar algunas sencillas reglas:

- **Cambiar las vocales por números**. Por ejemplo:
  - Mi familia es genial → M3 f1m3l31 2s g2n31l
- **Utilizar reglas mnemotécnicas**. Por ejemplo, elegir la primera letra de cada una de las palabras de una frase que sea fácil de recordar para nosotros:
  - Con 10 cañones por banda… → C10cpb…
- **Para hacer más sencillo el trabajo, podemos utilizar claves basadas en un mismo patrón, introduciendo ligeras variaciones para cada servicio**. Por ejemplo, tomando como base la contraseña anterior, añadir al final la última letra del servicio utilizado en mayúscula:
  - Facebook → C10cpb…K
  - Twitter → C10cpb…R
  - Gmail → C10cpb…L
- **Dependiendo del servicio y de su importancia podemos utilizar claves más robustas o menos, para facilitar su memorización.** Para los servicios más sensibles, siempre podemos utilizar un generador aleatorio de contraseñas. La mayoría de los gestores de contraseñas ofrecen esta funcionalidad.

> Otra razón para no utilizar la misma clave en diferentes servicios es el hecho de que **algunos** de ellos **no almacenan nuestra contraseña cifrada en sus servidores.** En este caso, involuntariamente la estamos compartiendo con estos servicios, por lo que debemos poner una contraseña que no se parezca a ninguna de las otras que utilizamos. Una pista **para poder identificar estos servicios es comprobar si al darnos de alta o recuperar la contraseña nos indican cual era nuestra clave**, en lugar de

> proporcionarnos un enlace para cambiarla.

Ayúdate de un gestor de contraseñas:

En la actualidad, manejamos distintas contraseñas para cada una de las actividades que realizamos: compras online, plataformas de streaming, correos electrónicos, gestiones bancarias.... todas y cada una han de ser distintas y cumplir unas condiciones muy particulares (mayúsculas, número de caracteres, con/sin símbolos...).

Por ello, los gestores de contraseñas se vuelven poderosos aliados ayudándonos a generar contraseñas tan seguras como aleatorias, y a tenerlas almacenadas para cuando nos son requeridas.

> Utiliza sólo gestores de contraseña en tus dispositivos personales y no en aquellos de uso público.

A continuación, encontrarás cinco gestores de contraseñas gratuitos y de código abierto:

- Keepass
- Bitwarden
- Passbolt
- Psono
- Teampass

Antivirus

Un antivirus es un software que protege nuestro dispositivo de programas malignos como **virus, spyware, gusanos, troyanos, rootkits**, etc. Además de **buscar y detectar** amenazas cuando se lo solicitamos, nos ofrecen **protección en tiempo real**.

Es imprescindible que estén siempre actualizados, por lo que se recomienda tener activada la **actualización automática** de modo que, cada vez que se inicie el ordenador, busque si hay actualizaciones pendientes y las instale.

Recuerda que el software malicioso no afecta sólo a los ordenadores, por lo que debes tenerlo instalado también en el resto de dispositivos que utilices (ej: smartphone)

Corta fuegos

La función del cortafuegos (o firewall, en inglés) es permitir, limitar, cifrar y descifrar el tráfico entrante en un sistema de información, bloqueando el acceso de personas o software externo no autorizado a nuestro ordenador y controlando también la información que diversos tipos de software puedan enviar desde nuestro ordenador, en sentido contrario.

Cuando un software es de confianza y requiere enviar y recibir información, debemos agregarlo a la lista de excepciones de nuestro cortafuegos.

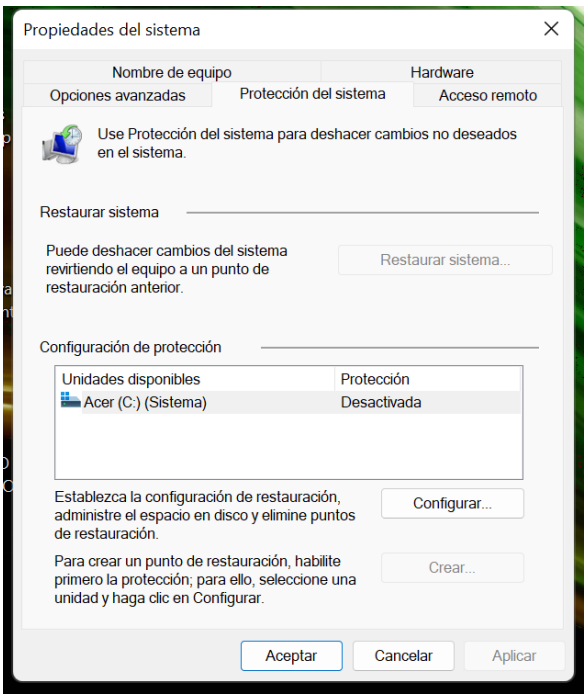
La protección del cortafuegos se limita únicamente a la información que viene a través de internet, no surtiendo efecto ante posibles infecciones por instalación local de software malicioso que pueda provenir, por ejemplo de un pendrive (en ese caso, el encargado de actuar es el antivirus).

Copias de seguridad

Ir haciendo copias de seguridad del material más importante es una buena manera de prevenir la pérdida de esta información si se diera una infección. Podemos recurrir a unidades extraíbles (USB, DVD, CD-R o CDRW) o al almacenamiento en la nube.

Otra opción es trabajar directamente en la nube con sus pros y sus contras:
Ventajas: No tendrás que estar almacenando las cosas regularmente pues dispone de autoguardado y sistema propio de Antivirus.
Desventajas: Requiere de conexión a Internet

Además, los sistemas operativos tienen la opción de programar puntos de restauración que nos permiten volver a tener nuestro PC como se encontraba en una fecha determinada.



> Algunas infecciones pueden deshabilitar la opción de restaurar el sistema del sistema operativo.

Mantente siempre actualizado

Parafraseando a Batman: "el mal no descansa", los hackers encuentran constantemente fallas de seguridad o hacen "mutar" a sus creaciones víricas. Es por esto que, los sistemas de seguridad

deben estar siempre actualizados y, con esto, no nos referimos únicamente a los antivirus. Esto es aplicable también a todo el software que utilicemos con acceso a internet como navegadores y, sobre todo, nuestro sistema operativo.

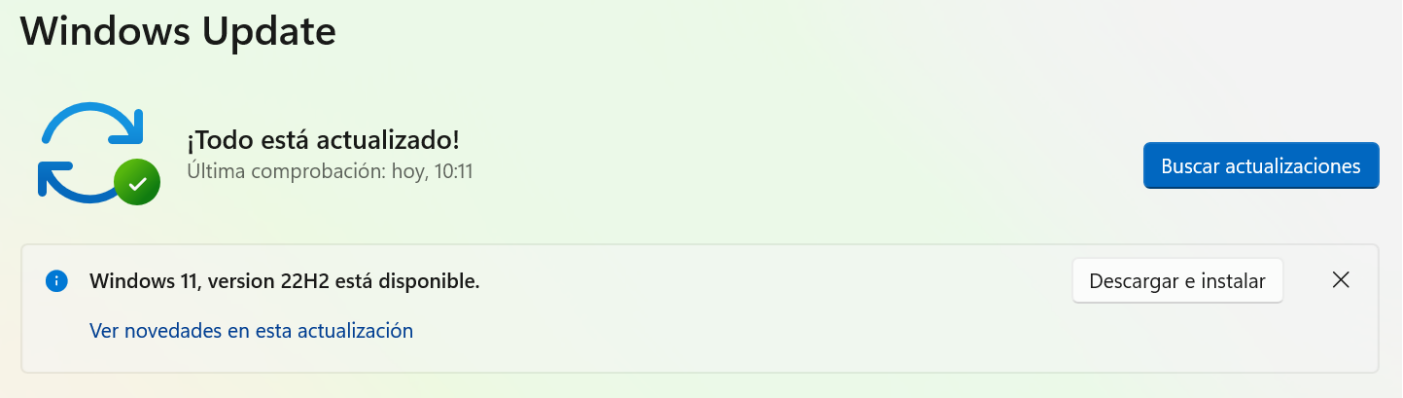


Ilustración: Buscar actualizaciones en Windows 11.

Utiliza distintas cuentas de usuario

El disponer de distintas cuentas de usuario y distintos permisos, también protegerá nuestros datos, sobre todo cuando utilicemos dispositivos compartidos.

Además de esto, las cuentas de un dispositivo pueden tener distintos roles y permisos:
Administrador: debe tener contraseña y ser la única con permisos para instalar aplicaciones, así como para configurar y actualizar el equipo.
Cuenta estándar: para el uso básico del equipo, pueden tener contraseña y se recomienda una por usuario que utilice el dispositivo regularmente. En ella pueden disponer de su configuración y sus carpetas de almacenamiento.
Cuenta invitado: para usuarios no habituales del equipo.

> Cuando estemos navegando en dispositivos que no son nuestros, es altamente recomendable utilizar el modo de incógnito, para no dejar datos de nuestra navegación tales como historial de navegación, contraseñas, caché...

Finalmente, hay cuentas reservadas a menores, o **herramientas de control parental** que pueden ser útiles para bloquear páginas y aplicaciones, limitar el tiempo de uso o generar informes de uso para los tutores de las criaturas.

El sentido común, el más común de los sentidos

Y es que no es más limpio el que más limpia, si no el que menos ensucia. Por mucho software de protección que tengamos, puntos de restauración o contraseñas seguras, si nuestro comportamiento no es prudente estaremos condenados a una infección. A continuación, vamos a

dar una serie de consejos a tener en cuenta:

1. **Desconfía de mensajes y correos de remitentes desconocidos.** Estos pueden tener invitaciones u ofertas dudosas. En ocasiones presentan incongruencias gramaticales por estar traducidos automáticamente.
2. **No compartas datos personales ni sensibles** con remitentes desconocidos.
3. **Evita las cadenas de mensajes**, ya que además de tener un contenido más que cuestionable, son repositorios de direcciones que pueden utilizarse con otros fines.
4. **Evita utilizar redes Wi-Fi públicas abiertas**: ya que estas son utilizadas por hackers para acceder a información de aquellos que se conectan.

Revision #7
Created 31 December 2022 11:30:24 by Fran Mentoría Huesca
Updated 24 February 2023 10:57:55 by Paola G